CORPORATE DATA PRIVACY & PROTECTION POLICY

Comprehensive Security, Governance, and Global Compliance Framework

This document establishes the comprehensive operational mandates, technical safeguards, and legal frameworks governing data processing, client asset protection, and privacy management at WebStride Solutions. This policy is binding for all internal operations, international client engagements, and cross-border digital transformations.

Organization	WebStride Solutions
Document Reference	WSS-DPPP-2026-V1
Effective Date	May 20, 2026
Compliance Mandates	Kenya Data Protection Act (2019), General Data Protection Regulation (GDPR), International Privacy Standard ISO/IEC 27701
Target Audience	Corporate Clients, Global Partners, Technical Personnel, Supervisory Authorities
Classification	Public / Client-Facing Governance Framework

TABLE OF CONTENTS

This policy framework is organized into the following operational and legal sections:

1. DOCUMENT CONTROL & AUTHORIZATION FRAMEWORK

WebStride Solutions operates under rigid institutional controls to ensure data protection mechanisms remain current, legally resilient, and operationally integrated. This section specifies the governance baseline for this policy document.

1.1 Version Control Ledger

Version	Date of Issue	Primary Authors / Reviewers	Operational Status
v1.0	May 20, 2026	Executive Directorate & Legal Counsel	Active / Authorized Standard

1.2 Institutional Approval

This regulatory policy has been evaluated, approved, and enacted by the executive governance board of WebStride Solutions. All operational units, including technical development, digital design, marketing systems, and strategic analysis, are strictly bound to enforce the directives herein. Non-compliance results in immediate administrative and civil interventions.

2. EXECUTIVE COMMITMENT & SCOPE OF APPLICATION

At WebStride Solutions, data integrity is recognized as a fundamental element of enterprise trust and digital operational excellence. As a modern digital agency leading large-scale technological implementations, we understand that data privacy cannot be an afterthought—it must be deeply embedded into every pixel, system integration, and marketing methodology we deploy.

Our global corporate clients entrust us with proprietary workflows, system keys, enterprise databases, and direct lines of customer interaction. This policy outlines our absolute transparency regarding information collection, storage protocols, protective systems, and decommissioning frameworks.

2.1 Omnidirectional Scope of Application

This Data Privacy and Protection Policy applies universally to all business operations executed by WebStride Solutions, regardless of geographical location, communication channel, or operational jurisdiction. The scope comprehensively encompasses:

- **Domestic Client Frameworks:** All activities, projects, and entities operating inside Kenya, managed in strict conformance with local statutory regimes.

- **International Client Frameworks:** Cross-border data transactions, cloud migrations, and global marketing frameworks touching data subjects in the European Union, Americas, and pan-African trade blocks.
- **Internal Structural Data:** Proprietary tools, platform environments, analytics processing, and staging platforms used by WebStride Solutions personnel to coordinate project delivery.

Operational Maxim: WebStredi Solutions enforces a strict "Security by Design and by Default" operational philosophy. No project, repository, or campaign is authorized for deployment without an explicit evaluation of its data privacy impacts.

3. LEGISLATIVE AND REGULATORY ALIGNMENT FRAMEWORK

WebStride Solutions operates a legally unified compliance model that cross-references and actively integrates the strictest global and local statutory regulations. By standardizing our practices against diversified international architectures, we guarantee an uncompromised baseline of protection for both domestic and overseas corporate clients.

3.1 The Kenya Data Protection Act (2019)

As an entity headquartered and operating within the Republic of Kenya, WebStride Solutions fully aligns its data systems with the requirements of the Office of the Data Protection Commissioner (ODPC). In compliance with the Kenya Data Protection Act (2019), we enforce the core tenets of lawful processing, minimization, purpose limitation, and strict local/cross-border transmission controls under the statutory mandates of the Act.

3.2 The General Data Protection Regulation (GDPR)

To accommodate our extensive international clientele and global market reach, our internal systems structurally implement the requirements of Regulation (EU) 2016/679 (GDPR). For all processing containing data associated with European subjects, WebStride Solutions acts as a robust Data Processor or Joint Controller, upholding international data export protections, executing formal contractual clauses, and honoring individual subject rights seamlessly.

3.3 Complementary Transnational Frameworks

Where applicable, our operations adapt dynamically to standard international models, including the California Consumer Privacy Act (CCPA) and South Africa’s Protection of Personal Information Act (POPIA), ensuring complete interoperability across all modern digital borders.

4. DEFINITIONS & STATUTORY LEGAL INTERPRETATIONS

To ensure absolute semantic clarity among our partners, legal counsels, and technical teams, the following statutory interpretations are applied throughout this document:

Personal Data: Any information relating to an identified or identifiable natural person (Data Subject), directly or indirectly, via identifiers such as name, identification numbers, geolocation coordinates, or digital identity markers.

Sensitive Personal Data: Data revealing properties such as financial status, identity profiles, genetic records, health conditions, or confidential corporate authentication credentials.

Data Controller: The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Data Controller. WebStride Solutions frequently serves as a Data Processor when managing digital properties for clients.

Elevated System Access: Access privileges encompassing administrative, root, or API-level credentials allowing deep structural entry into live client social networks, website backends, cloud hostings, database engines, or financial hubs.

5. DATA COLLECTION ARCHITECTURE & TAXONOMY

WebStride Solutions restricts its data collection infrastructure exclusively to information necessary for the execution of enterprise-grade technical contracts, optimization workflows, and marketing communication pipelines. We do not engage in unauthorized scraping or unverified third-party data acquisitions.

5.1 Taxonomy of Collected Information

Categor y	Specific Data Elements Collected	Lawful Basis for Processing
Corporate Client Data	Names, corporate emails, physical headquarters details, registration certificates, tax identifiers, billing records.	Contractual necessity / Performance of Core Agreement.

Operational Credentials	OAuth tokens, administrative logins, CMS access records, Meta Business Manager keys, API strings, FTP configurations.	Explicit Client Authorization and Contractual Mandate.
Public Interaction Analytics	IP addresses, device finger-prints, cookie identifiers, geographic nodes, session parameters, bounce vectors.	Legitimate Business Interest / Informed User Consent.
Inbound Lead Assets	Form submissions, newsletter email records, marketing preferences, business profile data sheets.	Explicit Opt-In Consent.

5.2 Data Minimization Protocols

WebStride Solutions structurally applies an algorithmic data minimization methodology across all digital projects. The volume of data ingested is governed by the relation:

$$D_{ingest} \leq \sum (S_{critical} + L_{mandated})$$

Where $S_{critical}$ represents the absolute minimal technical variables required to execute the specific scope of service, and $L_{mandated}$ represents local regulatory or legal data logging requirements. Any data point outside this envelope is rejected at entry point.

> **Critical Notice:** Clients are explicitly requested to provide system access exclusively through the designated, isolated channels outlined in Section 7 of this document. Credentials must never be transmitted via insecure platforms such as standard email or unencrypted instant messaging applications.

6. CORE SERVICE-SPECIFIC DATA LIFECYCLES

Because our agency provides highly diversified technical solutions, data management must adapt specifically to the technological reality of each individual service pipeline. Below is our operational model categorized by core service line.

6.1 Web Design & Development Environments

During high-performance web development cycles, WebStride Solutions interacts directly with enterprise staging environments, raw source code repositories, databases, and hosting infrastructures.

- **Staging Protocols:** All development cycles are isolated within secure sandboxed environments using dummy data sets. Production data pipelines are never mapped directly into development environments.

- **API Integration Safety:** Third-party APIs (payment pathways, CRM endpoints, map layers) are restricted using strict IP whitelisting and encrypted environmental variable stores.
- **Framework Standardization:** Web builds utilize secure frameworks incorporating automated cross-site scripting (XSS) prevention, SQL injection blocks, and forced HTTPS/TLS routing layers.

6.2 Corporate Graphic Design Asset Pipelines

Graphic and brand identity generation requires the storage and cataloging of proprietary asset designs, corporate visual guidelines, product mockups, and strategic brand files.

- **Storage Security:** Creative files, vectorized internal templates, and high-fidelity project boards are housed in encrypted cloud-storage buckets accessible only by assigned designers.
- **Intellectual Integrity:** All intermediate assets and rejected drafts remain structurally locked and isolated to prevent leakage before official public market launches.

6.3 Search Engine Optimization (SEO) & Technical Auditing

SEO execution requires integration with deep platform diagnostics including Google Search Console, Google Analytics, competitive visibility metrics, and internal indexing frameworks.

- **Data Handling Limits:** Analytics data extracted for performance reporting is treated with confidentiality. We ensure that raw client audience streams are aggregated and processed without revealing individual end-user identities.
- **Audit Tracking:** Crawler software used to perform architectural code reviews is configured to operate at safe crawl speeds, preventing denial-of-service issues on live business infrastructure.

6.4 High-Access Social Media Management Frameworks

Social media management involves handling live, public-facing digital communication assets. This is our highest exposure service area, demanding strict governance.

- **Zero-Password Sharing Policy:** Social media networks (Meta Business Suite, LinkedIn Page Admin, X Pro, TikTok for Business) are accessed using programmatic delegation (e.g., Partner Access allocations) rather than raw username-and-password distribution.
- **Content Pre-Approval Architecture:** All marketing posts, audience engagements, and campaigns are managed via isolated software systems with strict permission controls. No content is pushed live without passing automated verification and client digital sign-off protocols.

7. CREDENTIALS SECURITY & ELEVATED ACCESS PROTOCOLS

Managing complex platforms requires handling sensitive authentication systems. WebStride Solutions enforces strict rules to prevent credential misuse or accidental exposure.

7.1 Enterprise Password Vaulting and Infrastructure

Under no circumstances are WebStride Solutions personnel permitted to write down, store locally, or share client passwords inside unencrypted formats (such as text files, internal group chats, or notebooks).

- **Vault Centralization:** All access tokens, secondary API keys, and administrative credentials are secured within a centralized, enterprise-tier, zero-knowledge encrypted password management system.
- **Multi-Factor Mandate:** Every access portal to our internal tools requires mandatory Multi-Factor Authentication (MFA), combining time-based one-time tokens (TOTP) with strict hardware/device checks.
- **Session Isolation:** Sessions on client platforms are conducted via secure, containerized browser instances that clear cache and operational history automatically upon logout.

7.2 Revocation and Auditing Framework

Access permissions follow a strict "Least Privilege Model." Team members are granted access exclusively to platforms necessary for their specific tasks. Upon employee offboarding or shifting project assignments, all associated system keys are automatically rotated, and platform permissions are immediately revoked.

8. WEBSITE INTERACTIVITY, COOKIES, & BEHAVIORAL TRACKING

When individuals visit the official WebStride Solutions platform or interact with digital properties deployed by our team, certain information is collected automatically using programmatic tracking networks.

8.1 Cookie Governance and Classification

Our website utilizes cookies and similar web technologies to monitor user interactions and deliver personalized digital experiences. Cookies are categorized as follows:

- **Strictly Necessary Cookies:** Essential for standard website operation, security checking, load balancing, and functional stability. These do not require user consent.

- **Performance & Analytics Cookies:** Gather anonymous operational data on user navigation paths, loading speeds, and overall technical performance to guide optimization efforts.
- **Marketing & Retargeting Cookies:** Track multi-platform interaction states, allowing WebStreet Solutions to deliver relevant advertising notifications across search engines and social platforms.

8.2 Marketing Notification and Opt-Out Mechanism

Inbound marketing distributions, digital newsletters, or technology insight updates are sent exclusively to users who have provided explicit opt-in consent. Every communication contains a single-click, automated unsubscription link allowing instantaneous opt-out from further marketing communications.

Tracking Technology	Primary Purpose	User Control Mechanism
Google Analytics Tag	Aggregated user experience reporting, session mapping, geographic tracking.	Cookie Consent Banner / Browser Opt-Out Extensions.
Meta Pixel Integration	Measuring campaign efficiency and delivering relevant retargeting ads.	Social Profile Ad Settings / Cookie Preference Center.

9. FINANCIAL SECURITY & TRANSACTION INTEGRITY STANDARD

Financial records and payment interactions demand maximum security. WebStride Solutions maintains an isolated environment for transaction handling, ensuring that no client financial details are exposed.

9.1 Compliance with Financial Standards

Our agency integrates with tier-one, internationally certified payment gateways and processing systems. All online invoice fulfillments, banking transactions, and cross-border digital wire compliance follow the Payment Card Industry Data Security Standard (PCI-DSS).

9.2 Isolation of Credit Card and Account Information

WebStride Solutions servers never store, process, or transmit raw credit card primary account numbers (PAN), CVV strings, or bank account authorization codes. Financial interactions occur through encrypted iframe overlays managed directly by the certified payment vendor. Internal accounting records retain only reference tokens and necessary transactional summaries for tax and financial auditing purposes.

10. DATA SHARING, MANDATED LEGAL DISCLOSURES, & THIRD-PARTY RULES

WebStredi Solutions does not sell, rent, trade, or distribute client data to third-party data brokers or external commercial operations under any circumstances. Data sharing is limited to the narrow conditions defined below.

10.1 Government and Sovereign Authority Disclosures

We may disclose personal or operational data to sovereign regulatory structures, national law enforcement bureaus, or judicial courts only when compelled by a valid legal order, such as a formal subpoena, court warrant, or official directive issued by a competent regulatory authority (e.g., the Kenya Data Protection Commissioner or an authorized international equivalent).

Our internal legal counsel evaluates all disclosure demands to ensure full compliance with the following protocol:

Legal Verification Protocol: Upon receipt of a data disclosure request from a government body, WebStride Solutions will assess the order's validity. Unless strictly prohibited by national security legislation or a judicial gag order, **the affected client will be notified within twenty-four (24) hours** to allow them to seek appropriate legal protection.

10.2 Client-Authorized Disclosures

Data sharing may occur when a client explicitly requests integration with third-party software vendors, external consultants, or independent contractor teams. WebStride Solutions requires a written authorization matrix from the client before transferring operational data outside our system boundaries.

10.3 Essential Vendor Sub-Processing

To deliver our digital services, we partner with reliable cloud sub-processors (including enterprise cloud hosts, CDN nodes, and transactional mail servers). All sub-processors are vetted for strict alignment with the data privacy principles established in this policy.

11. DATA RETENTION, STRUCTURAL ARCHIVING, & PURGING LIFECYCLE

WebStride Solutions implements clear lifecycle controls for all data in our custody. Information is preserved only for as long as necessary to fulfill project requirements, meet regulatory tracking needs, or protect vital business records.

11.1 The Five (5) Year Contractual Archive Rule

Following the formal conclusion, termination, or natural expiration of a commercial service contract with a client, all related data assets enter a locked, post-contract archival status.

WebStride Solutions enforces a strict **five (5) year retention period** from the exact date of contract conclusion. This archive period is required to support:

- **Regulatory and Tax Compliance:** Meeting local corporate recordkeeping mandates under Kenyan and international tax laws.
- **Legal Defensibility:** Ensuring necessary evidence remains available for potential commercial disputes, contractual reviews, or audits.
- **Business Continuity:** Providing an archival recovery window should the client return to reactivate or upgrade their digital properties.

11.2 Complete and Permanent System Deletion

Upon reaching the exact five-year anniversary of contract termination, WebStride Solutions initiates an automated and manual data decommissioning workflow. The data is permanently purged and cannot be recovered.

- **Database Deletion:** All associated database entries, client tracking rows, and operational profiles are completely erased from our active and passive production systems.

- **File Destruction:** Digital files, design assets, website backups, and development repositories are overwritten using secure file deletion methods to prevent forensic recovery.
- **Backup Overwriting:** Long-term offline or cold-tier backups are left to expire and overwrite naturally through our rotational backup architecture within a maximum of ninety (90) days from the initial deletion command.

12. STATUTORY RIGHTS OF DATA SUBJECTS & ENFORCEMENT

We respect the statutory legal rights granted to data subjects under both the Kenya Data Protection Act (2019) and the General Data Protection Regulation (GDPR). WebStride Solutions provides clear mechanisms for individuals to exercise their privacy choices.

12.1 Matrix of Subject Rights

- **Right to Affirmation and Access:** Data subjects may request clear confirmation regarding whether their personal information is actively being processed, along with a readable copy of that data.
- **Right to Rectification:** The right to demand immediate correction of incomplete, inaccurate, or outdated personal information.
- **Right to Erasure ("Right to be Forgotten"):** The right to request the total deletion of personal data where there is no longer a valid legal basis or contractual requirement for its retention.
- **Right to Data Portability:** The right to receive personal data in a structured, commonly used, and machine-readable format for transfer to another digital provider.
- **Right to Object to Processing:** The right to object at any time to the processing of personal data for direct marketing or automated profiling.

12.2 Request Execution and Verification

To execute any statutory right, the data subject must submit a formal request to our privacy office (details in Section 14). We apply strict verification procedures to confirm the requester's identity before processing the request, protecting against unauthorized data access. Verified requests are resolved within thirty (30) days without charge.

13. TECHNICAL & ORGANIZATIONAL SECURITY MEASURES (TOMS)

To ensure data remains secure against unauthorized access, accidental alteration, or catastrophic loss, WebStride Solutions maintains an updated framework of Technical and Organizational Measures (TOMs).

13.1 Cryptographic Controls

Data handled by WebStride Solutions is protected by robust encryption standards across all lifecycles.

- **Data in Transit:** All data moving across network channels is encrypted using Transport Layer Security (TLS 1.3) protocols.
- **Data at Rest:** Enterprise storage systems, local workstations, and cloud databases deploy Advanced Encryption Standard (AES-256) encryption keys.

13.2 Administrative and Workspace Protections

Security is integrated into our daily workplace operations and organizational culture.

- **Confidentiality Agreements:** Every WebStride Solutions employee and contractor signs a comprehensive, legally binding Non-Disclosure Agreement (NDA) before accessing any client system.
- **Continuous Training:** Personnel complete mandatory bi-annual security awareness workshops covering social engineering protection, secure coding practices, and identity access safety.
- **Endpoint Protection:** Company devices run centralized endpoint detection and response (EDR) software, use encrypted drives, and enforce automatic inactivity timeouts.

14. BREACH NOTIFICATION, INCIDENT HANDLING, & CONTACT ARCHITECTURE

WebStride Solutions maintains an operational Data Incident Response Team (DIRT) trained to manage potential security compromises quickly and effectively.

14.1 Incident Management and Mandatory Reporting Timeline

In the event of a verified security compromise leading to unauthorized access, alteration, loss, or disclosure of data, WebStride Solutions initiates its incident response protocol.

If the incident poses a risk to the rights and freedoms of individuals, WebStride Solutions will fulfill all regulatory reporting requirements:

> **Regulatory Reporting Mandate:** We will notify the Office of the Data Protection Commissioner (ODPC) in Kenya, along with relevant international supervisory bodies, **within seventy-two (72) hours** of breach verification. Affected clients will be notified immediately to ensure coordinated risk mitigation.

14.2 Direct Privacy Contact Point

For inquiries regarding this Data Privacy and Protection Policy, statutory rights execution, or data security audits, please contact our dedicated data protection office:

Office of Data Privacy and Compliance

WebStride Solutions

Email Contact: privacy@webstreetsolutions.com

Mailing Address: Nairobi, Kenya

Operational Scope: International Privacy and Technical Security Operations

14.3 Continuous Policy Maintenance

This policy framework is reviewed annually to adapt to shifting technological capabilities, changes in our agency service lines, and emerging global data protection regulations. Updates are logged in our central document tracking ledger and shared with active clients.